UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,329	06/27/2001	Marcus Peinado	MSFT-164268.1	1912

41505 7590 08/10/2005

WOODCOCK WASHBURN LLP
ONE LIBERTY PLACE - 46TH FLOOR
PHILADELPHIA, PA 19103

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 08/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/892,329	PEINADO ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *15-18,20-27,31-34 and 36-43* is/are pending in the application.

4a) Of the above claim(s) *1-14, 28-30, and 44-46* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15-18,20-27,31-34 and 36-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's arguments/amendments with respect to canceled claim 1-14, 28-30, and 44-46, amended claims 15 and 31, and currently pending claims 15-18, 20-27, 31-34, and 36-43, filed on July 11, 2005 have been fully considered but they are not persuasive. The examiner would like to point out that this action is made final (MPEP 706.07a).

Response to Arguments

2. Applicant argues that:

a. Independent claims 15, and 31are not taught by Vu to include *"the security kernel employs the accessed security key during the preferred mode to authenticate/verify the application prior to instantiation thereof, and also authentication of any application is not disclosed by Vu"(page 16 last paragraph).*

b. Vu fails to support claim 25 and 41, wherein *"to choose and instantiate one of a plurality of applications on a secure processor, and switching between modes as recited to first load and then operate a chooser application, employ same to select a chooser value corresponding to a chosen application, and then load and operate a chosen application"* (page 18 par. 3).

c. Dependent claims 16-18, 20-24, 26-27, 32-34, 36-40, and 42-43 are allowable based upon their dependency on allowable claims 15, 25, 31, and 41 (page 17 par. 3 and page 19 par. 1).

However, Examiner disagrees with applicant.

Regarding argument (a), Argument is not persuasive. Vu teaches a method and apparatus for secure processing of cryptographic keys using a secure/preferred processor mode, which cannot be interrupted/accessed by other interrupters to read/access ciphered cryptographic key in order to use the ciphered cryptographic key for authentication of documents/contents (decrypting content applications) sent over public network, users to allow privileged access, secure online electronic commerce, confidential information, access control (col. 1 lines 11-29, and col. 5 lines 35-40), and any applications which requires some secret information (col. 2 lines 19-20). Argument is not persuasive because, ciphered key is accessed first in a secure mode and application is authenticated/decrypted in using the key. In other words the accessed key is used for application and/or application is authenticated/decrypted after accessing the key.

Regarding argument (b), Argument is not persuasive. Vu discloses plurality of applications/documents as mentioned above. In addition, Vu's method is used for protecting contents/applications sent over public network (see, col. 1 lines 11-29, and col. 2 lines 19-20). When a user chooses to instantiate an application, the processor is

initialized to a secure mode, encrypted cryptography key is accessed and application is authenticated (col. 4 lines 12-39 and col. 5 lines 25-47).

Regarding argument (d), examiner disagrees with applicant. Based on the arguments set forth by the examiner for arguments (a), and (b), the dependent claims stand rejected.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. Therefore, the examiner asserts that the system of the prior art, Vu does teach or suggest the subject matter as recited in independent claims 15, 25, 31, and 41. Dependent claims 16-18, 20-24, 26-27, 32-34, 36-40, and 42-43 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action dated August 5, 2005. Accordingly, rejections for claims 15-18, 20-27, 31-34, and 36-43 are respectfully maintained.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

4. Claims 15-18, 20-27, 31-34, and 36-43 are rejected under 35 U.S.C. 102(e) as being anticipated by Vu et al. (Vu, Patent No.: US 6,557,104 B2).

As per claim 15 and 31, Vu teaches a method/medium for a secure processor to instantiate and authenticate a secure application thereon by way of a security kernel, the method comprising:

entering a preferred mode where a security key of the processor is accessible (Vu col. 5 lines 25-35);

instantiating and running a security kernel, the security kernel:

accessing the security key (Vu col. 5 lines 35-36);

applying the accessed security key to decrypt at least one encrypted key for the application (Vu col. 5 lines 35-40);

storing the decrypted key(s) in a location where the application will expect the key(s) to be found (Vu col. 6 lines 65-col. 7 lines 11); and

authenticating the application on the processor (Vu col. 5 lines 36-40, and col. 7 lines 7-11); and

entering a normal mode from the preferred mode after the security kernel authenticates the application (Vu Fig. 2 No. 25 and col. 5 lines 42-47),

where the security key is not accessible; wherein the security kernel allows the processor to be trusted to keep hidden the key(s) of the application (Vu col. 4 lines 63-col. 5 lines 9); and

wherein the security kernel employs the accessed security key during the preferred mode to authenticate/verify the application prior to instantiating thereof (Vu col. 5 lines 35-40).

As per claim 25 and 41, Vu teaches a method/medium for a secure processor to instantiate one of a plurality of available secure applications thereon by way of a security kernel, the method comprising:

setting a chooser value to a value corresponding to a chooser application upon power-up (Vu col. 4 lines 12-39, and col. 5 lines 1-4 and18-20);

entering a preferred mode upon a power-up CPU reset and instantiating the security kernel, the security kernel determining that the chooser value corresponds to the chooser application and therefore authenticating same, the chooser application being instantiated (Vu col. 4 lines 52-col. 5 lines 8, and col. 5 lines 36-40);

entering a normal mode after the chooser application is instantiated and leaving same to run, the chooser application presenting the plurality of available applications for selection by a user (Vu col. 5 lines 40-44 and fig. 2 No. 25);

receiving a selection of one of the presented applications to be instantiated (Vu col. 5 lines 32-40);

setting the chooser value to a value corresponding to the selected application (Vu col. 4 lines 12-39 and page 5 lines 18-20);

entering a preferred mode upon an executed CPU reset and instantiating the security kernel, the security kernel determining that the chooser value corresponds to the selected application and therefore authenticating same, the selected application being instantiated (Vu col. 4 lines 52-col. 5 lines 8 and col. 5 lines 36-40);

entering a normal mode after the selected application is instantiated and leaving same to run (Vu col. 5 lines 40-44 and fig. 2 No. 25);

wherein the security kernel allows the processor to be trusted to keep hidden a secret of the chooser application and a secret of the selected application (Vu col. 4 lines 63-col. 5 lines 29).

As per claims 16 and 32, Vu teaches the method/medium wherein entering the preferred mode comprises entering the preferred mode upon a CPU reset (Vu col. 4 lines 12-39 and col. 5 lines 18-20).

As per claims 17 and 33, Vu teaches the method/medium further comprising erasing data in a cache of the processor prior to instantiating the security kernel (Vu col. 5 lines 59-63).

As per claims 18 and 34, Vu teaches the method/medium further comprising erasing data in a cache of the processor after entering normal mode (Vu col. 5 lines 42-47).

As per claims 19 and 35, Vu teaches the method/medium wherein the security kernel employs the accessed security key during the preferred mode to authenticate/verify the application prior to instantiation thereof (Vu col. 5 lines 35-40).

As per claims 20 and 36, Vu teaches the method/medium wherein the security kernel performs a hash/MAC (message authentication code) over at least a portion of the application and then compares the hash/MAC to a hash/MAC corresponding to the application (Vu col. 7 lines 1-11).

As per claims 21-22, and 37-38, Vu teaches the method/medium wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
MAC (main body, KMAN)	message authentication code of the main body under KMAN
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN (Vu col. 6 lines 64-65; encrypted encryption key);

computing MAC (main body, KMAN) (Vu col. 5 lines 32-40 and col. 7 lines 1-11);

comparing the computed MAC to MAC (main body, KMAN) from the header to determine if the code image has been changed (Vu col. 5 lines 32-40 and col. 7 lines 1-11); and

if the MACs match, applying KMAN to KMAN (KCODE) to produce KCODE (Vu col. 5 lines 32-40 and col. 7 lines 1-11).

As per claim 23, and 39, Vu teaches the method/medium wherein the security key of the processor is a private key of a public key--private key pair and the application is instantiated from a code image including a main body and a header including:

public key (KCODE)	KCODE encrypted according to the public key

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises applying the security key as the private key to public key (KCODE) to produce KCODE (Vu col. 7 lines 31-35).

As per claims 24 and 40, Vu teaches the method/medium wherein the security key of the processor is a private key of a public key-private key pair and the application is instantiated from a code image including a main body and a header including:

public key (HASH (main body), KCODE)	Hash of the main body and KCODE, both encrypted according to the public key

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

computing HASH (main body) (Vu col. 5 lines 32-40, col. 7 lines 1-11 and lines 31-35);

applying the private key to public key (HASH (main body), KCODE) to produce HASH (main body) and KCODE (Vu col. 5 lines 32-40, col. 7 lines 1-11 and lines 31-35);

comparing the computed HASH to the produced HASH to determine if the code image has been changed (Vu col. 5 lines 32-40, col. 7 lines 1-11 and lines 31-35); and

if the HASHs match, employing the produced KCODE as appropriate (Vu col. 5 lines 32-40, col. 7 lines 1-11 and lines 31-35).

As per claims 26 and 42, Vu teaches the method/medium further comprising setting the chooser value to the value corresponding to the chooser application upon the selected application being authenticated by the security kernel, wherein upon execution of a CPU reset, the security kernel determines that the chooser value corresponds to the chooser application 72c and therefore authenticates same (Vu col. 4 lines 12-39 and col. 5 lines 18-20).

As per claims 27 and 43, Vu teaches the method/medium further comprising storing the chooser value in a memory location not affected by a CPU reset so that the stored chooser value is available after same (Vu col. 5 lines 11-23).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw

August 5, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100